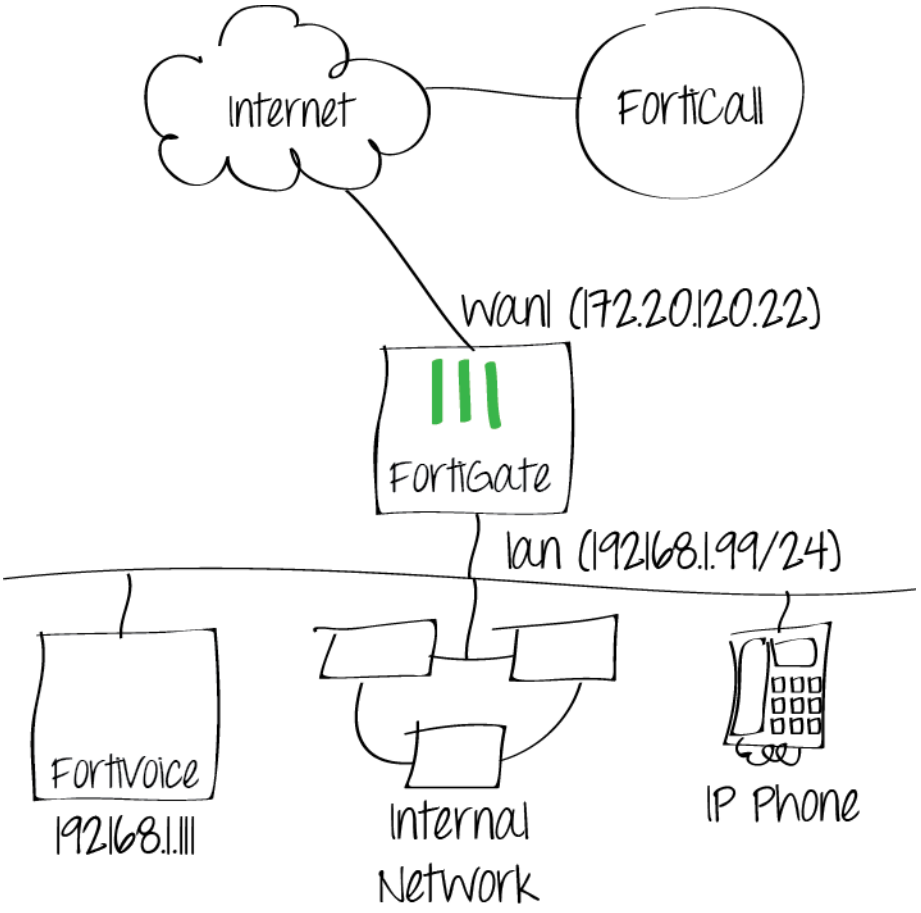
Allowing inbound and outbound VoIP/SIP traffic using FortiVoice and FortiCall

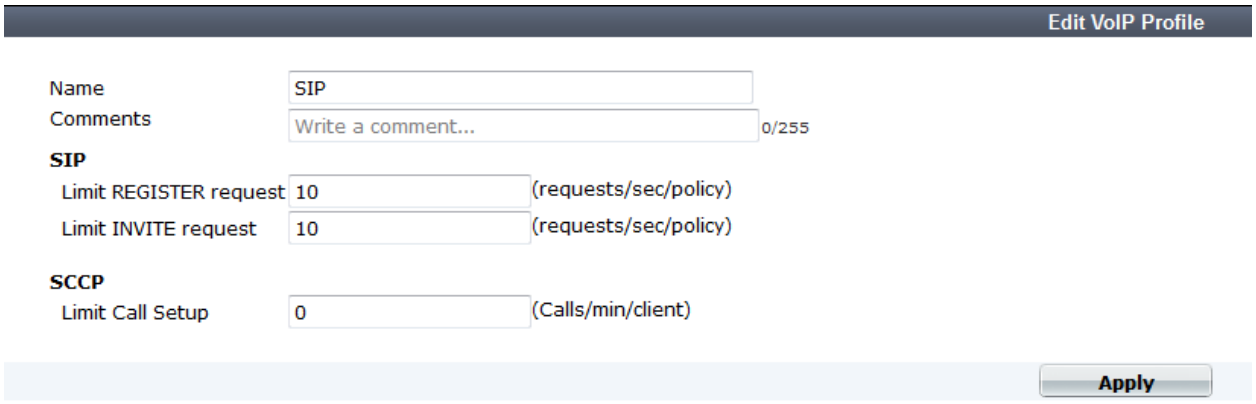
1. Network topology



This solution illustrate the steps to allow inbound and outbound SIP calls

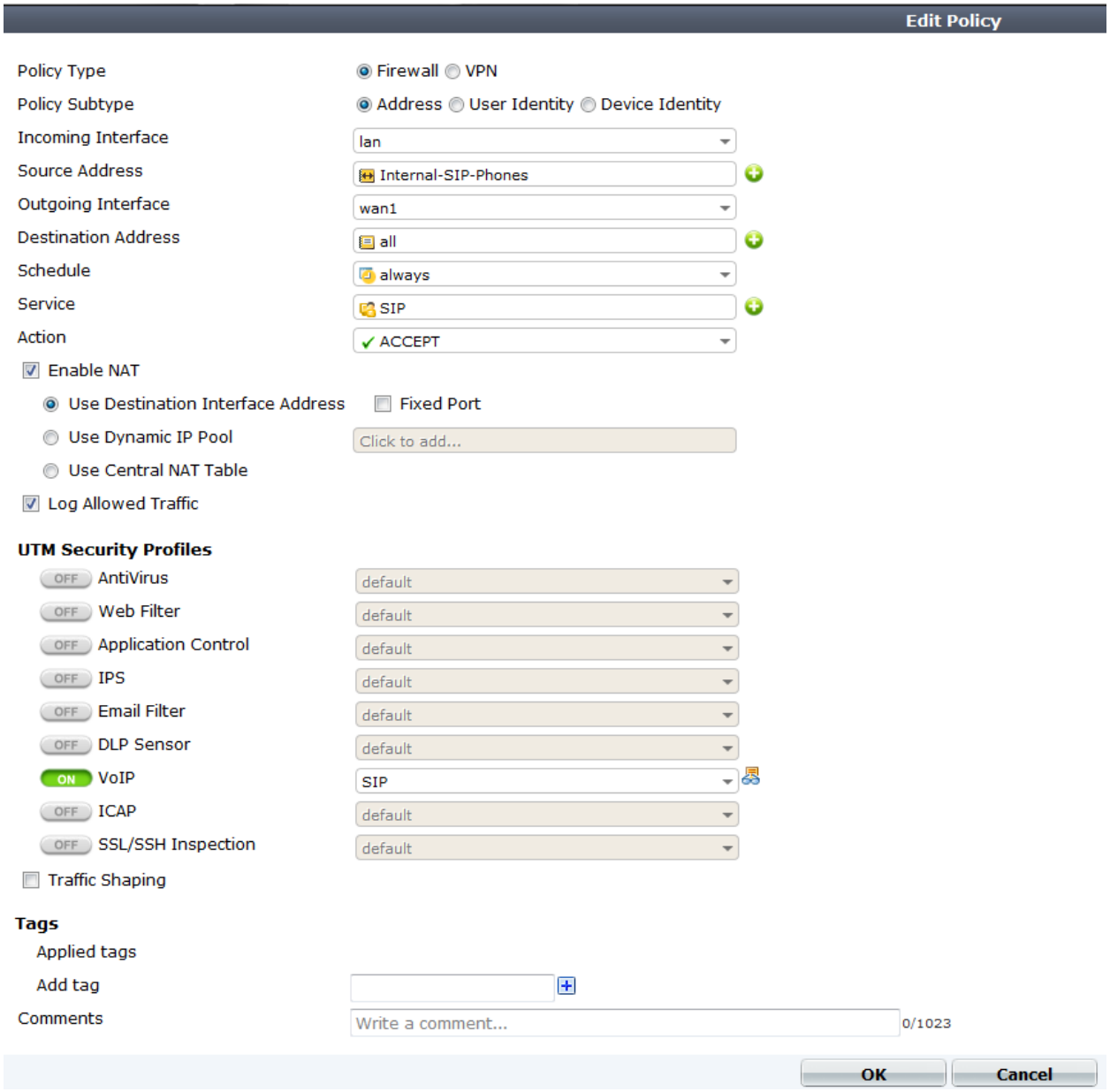
1. Configuring FortiGate for outbound SIP calls

Go to UTM Security Profiles > VoIP > Profile to create new and set the Limit REGISTER and INVITE requests



Go to Firewall Objects > Address > Address

Go to Policy > Policy > Policy

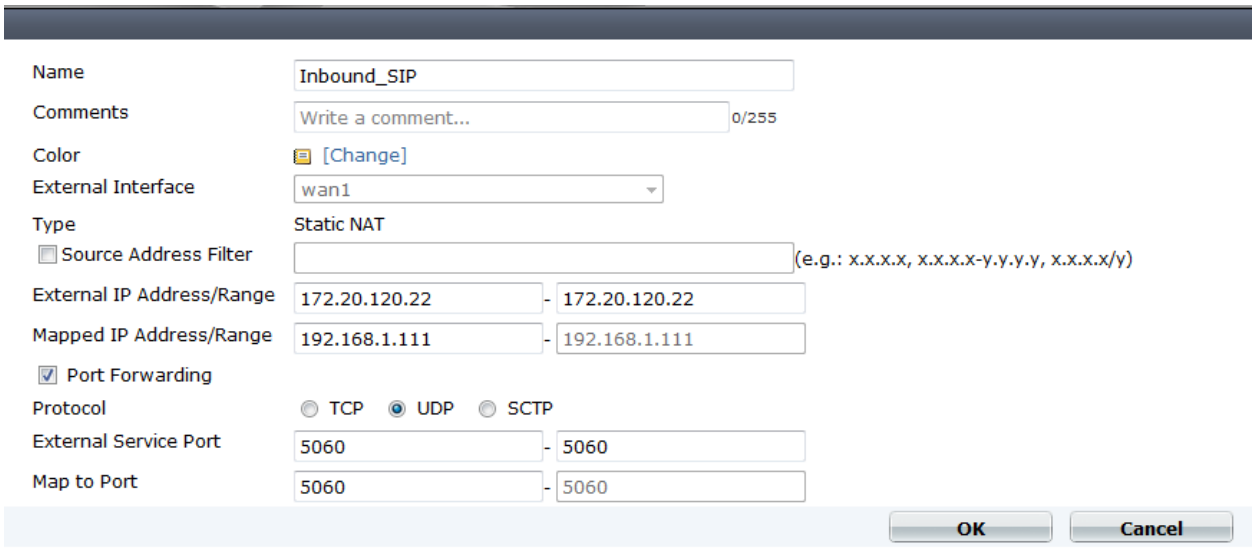


Make sure to turn ON VoIP and set SIP profile

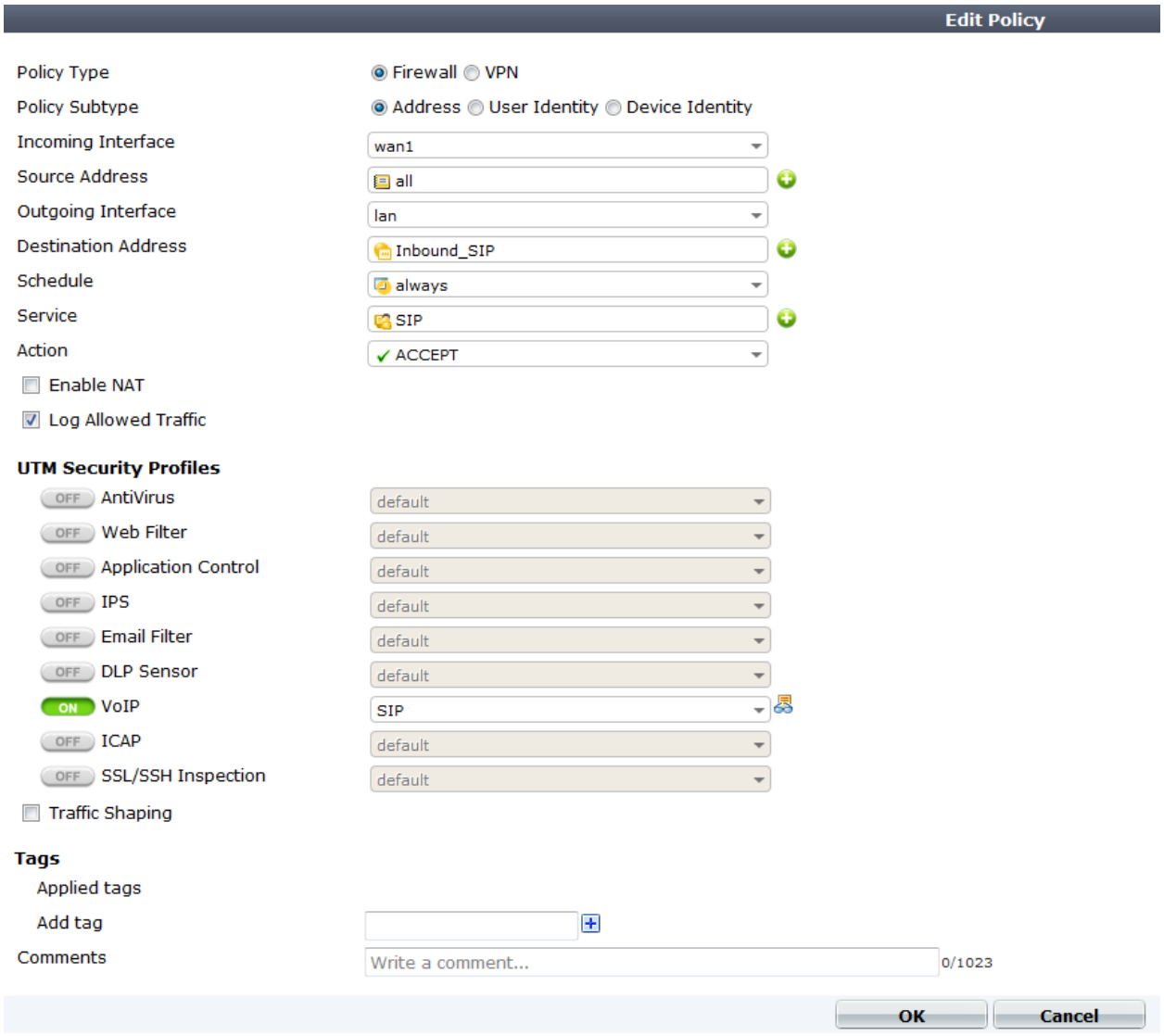
Make sure that this policy allowing outbound SIP traffic is on the top of the list

2. Configuring FortiGate for inbound SIP calls

Go to Firewall Objects > Virtual IP > Virtual IP to map the external IP on the wan1 interface of the FOrtiGate unit to the internal SIP Server (FortiVoice) IP on UDP port 5060



Go to Policy > Policy > Policy



3. Results

Go to System > Dashboard > Status > Widget and add “VoIP Usage” widget

Make in and out bound calls.

Go to System > Dashboard > Status to the SIP usage

VoIP Usage (Since 2013-01-30 10:44:02)

	SIP	SCCP
Voice Calls		
Currently Active Calls	0	0
Total Calls (since last reset)	5	0
Calls Failed/Dropped/Unanswered	0	0
Calls Succeeded	5	0

Go to Log & Report > Traffic Log > Forward Traffic and filter by policy id 2 and 3 (policy id 2 is for outbound SIP calls, policy id 3 is for inbound SIP calls)

Refresh | Download Raw Log | Log location: Disk

#	Date/Time	Src	Dst	Sent / Received	Policy ID	Service	UTM Action
1	11:52:03	66.11.10.43	172.20.120.22	574 B / 787 B	3	SIP	
2	11:51:33	192.168.1.111	66.11.10.43	14.79 KB / 20.84 KB	2	SIP	
3	11:44:46	66.11.10.43	172.20.120.22	44.65 KB / 34.70 KB	3	SIP	
4	11:15:55	66.11.10.43	172.20.120.22	40.69 KB / 31.42 KB	3	SIP	
5	10:56:39	192.168.1.111	66.11.10.43	110.16 KB / 107.42 KB	3	SIP	
6	10:53:26	66.11.10.43	172.20.120.22	2.20 KB / 1.70 KB	3	SIP	
7	10:52:04	192.168.1.111	66.11.10.43	15.10 KB / 19.15 KB	2	SIP	
8	10:46:56	192.168.1.111	66.11.10.43	205.27 KB / 201.37 KB	2	SIP	
9	08:27:31	66.11.10.43	172.20.120.22	4.64 KB / 3.97 KB	3	SIP	
10	08:25:35	66.11.10.43	172.20.120.22	6.29 KB / 5.34 KB	3	SIP	
11	08:24:06	192.168.1.111	66.11.10.43	215.43 KB / 215.04 KB	3	SIP	
12	08:22:18	192.168.1.111	66.11.10.43	1.37 MB / 1.77 MB	2	SIP	
13	06:31:04	192.168.1.111	66.11.10.43	97.27 KB / 95.51 KB	2	SIP	
14	01-29 11:44	66.11.10.43	172.20.120.22	2.76 KB / 2.04 KB	3	SIP	
15	01-29 11:41	66.11.10.43	172.20.120.22	2.49 KB / 2.28 KB	3	SIP	
16	01-29 11:40	192.168.1.111	192.168.1.99	113.28 KB / 113.09 KB	3	SIP	
17	01-29 11:36	192.168.1.111	66.11.10.43	6.71 KB / 7.93 KB	2	SIP	
18	01-29 11:31	192.168.1.111	66.11.10.43	22.95 KB / 30.72 KB	2	SIP	

Select an entry for each policy to see details

Dst	172.20.120.22	**Virtual Domain**	root
Received	787	**Source Country**	United States
Sent / Received	574 B / 787 B	**Dst NAT Port**	5060
Duration	29	**Sent**	574
Application Details		**Service**	SIP
Protocol	17	**Destination Country**	Reserved
Dst Port	5060	**roll**	65530
Status	✓	**Timestamp**	Wed Jan 30 11:52:03 2013
Tran Display	dnat	**Sequence Number**	11819
Policy ID	3	**Src Interface**	wan1
Src	66.11.10.43	**Dst NAT IP**	192.168.1.111
Sent Packets	1	**Level**	notice
Src Port	5060	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	2	**Date/Time**	11:52:03 (Wed Jan 30 11:52:03 2013)
Dst Interface	lan		

Dst	66.11.10.43	**Virtual Domain**	root
Received	21339	**Source Country**	Reserved
Src NAT IP	172.20.120.22	**Sent / Received**	14.79 KB / 20.84 KB
Duration	329	**Sent**	15147
Src NAT Port	5060	**Application Details**	
Service	SIP	**Protocol**	17
Destination Country	United States	**Dst Port**	5060
roll	65530	**Status**	✓
Timestamp	Wed Jan 30 11:51:33 2013	**Tran Display**	snat
Sequence Number	10829	**Policy ID**	2
Src Interface	lan	**Src**	192.168.1.111
Sent Packets	31	**Level**	notice
Src Port	5060	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	37	**Date/Time**	11:51:33 (Wed Jan 30 11:51:33 2013)
Dst Interface	wan1		